

PGCD – NOMBRES PREMIERS ENTRE EUX

1) PLUS GRAND COMMUN DIVISEUR : PGCD

A) DÉFINITION - PROPRIÉTÉS

Propriété – Définition :

Soit a et b deux entiers naturels non nuls.
Un entier naturel qui divise a et qui divise b est appelé **diviseur commun** à a et b .
L'ensemble des diviseurs communs à a et à b possède un plus grand élément que l'on appelle **le plus grand commun diviseur** de a et b , on le note $\text{PGCD}(a ; b)$.

Preuve :

Soit a et b deux entiers naturels non nuls. Considérons l'ensemble $D(a ; b)$, ensemble des diviseurs communs à a et b .
Le nombre 1 est un diviseur commun à a et b .
 $D(a ; b)$ est donc une partie non vide de \mathbb{N} .
De plus on sait que tout diviseur commun à a et b sera inférieur ou égal à a et à b .
Donc $D(a ; b)$ est une partie finie de \mathbb{N} .
 $D(a ; b)$ a donc un plus grand élément que l'on peut obtenir en rangeant dans l'ordre croissant (ou décroissant) les éléments de $D(a ; b)$.
C'est ce plus grand élément de $D(a ; b)$ qui est noté $\text{PGCD}(a ; b)$.

Exemples :

Dans \mathbb{N} l'ensemble des diviseurs de 15 est _____ et l'ensemble des diviseurs de 12 est _____

L'ensemble des diviseurs communs à 12 et à 15 est donc _____

Remarque :

a étant un entier naturel, l'ensemble des diviseurs de a est égal à l'ensemble des diviseurs de $-a$.
On pourra étendre, si besoin est, la notion de PGCD à des nombres entiers relatifs.

On dira par exemple que _____

Propriétés :

Soit a et b deux entiers naturels non nuls.	
• $\text{PGCD}(a ; b) \leq a$	• Si b divise a , on a $\text{PGCD}(a ; b) = b$
• $\text{PGCD}(a ; b) \leq b$	• $\text{PGCD}(a ; 1) = 1$
• $\text{PGCD}(a ; b) = \text{PGCD}(b ; a)$	• $\text{PGCD}(a ; a) = a$

Preuve :

- a étant un entier naturel, on sait que tous les diviseurs de a sont inférieurs ou égaux à a .
 $\text{PGCD}(a ; b)$ est un diviseur de a , donc $\text{PGCD}(a ; b) \leq a$
- On montre de même que $\text{PGCD}(a ; b) \leq b$
- Il est immédiat que les diviseurs communs à a et b , sont aussi les diviseurs communs à b et a . Donc $\text{PGCD}(a ; b) = \text{PGCD}(b ; a)$
- Si b divise a , alors b est un diviseur de a . Mais b est aussi un diviseur de b .
Donc b est un diviseur commun à a et b .
 $\text{PGCD}(a ; b)$ étant le plus grand des diviseurs communs à a et b , on a donc $\text{PGCD}(a ; b) \geq b$.
Or on a vu précédemment que $\text{PGCD}(a ; b) \leq b$
On en déduit : $\text{PGCD}(a ; b) = b$
- En prenant $b = 1$, et comme 1 divise a , on a $\text{PGCD}(a ; 1) = 1$ (résultat qui est par ailleurs évident)
- En prenant $b = a$, et comme a divise a , on a $\text{PGCD}(a ; a) = a$ (résultat qui est par ailleurs évident)

Exemple :

6 est un diviseur de 18 donc _____

B) ALGORITHME D'EUCLIDE

Propriété : Lemme d'Euclide

Soit a et b deux entiers naturels non nuls.
Soit q et r le quotient et le reste de la division euclidienne de a par b .
• Si $r = 0$, $\text{PGCD}(a ; b) = b$
• Si $r \neq 0$, $\text{PGCD}(a ; b) = \text{PGCD}(b ; r)$

Preuve :

a et b sont deux entiers naturels non nuls. q et r sont le quotient et le reste de la division euclidienne de a par b .
On a alors $a = b \times q + r$ avec $q \in \mathbb{N}$, $r \in \mathbb{N}$ et $0 \leq r < b$
• Si $r = 0$, alors $a = b \times q$ avec $q \in \mathbb{N}$, donc b divise a et par conséquent $\text{PGCD}(a ; b) = b$

- Si $r \neq 0$,
 - Considérons d un diviseur commun à a et b . On peut écrire $r = a - b \times q$
Comme d divise a et b , on en déduit que d divise r .
Donc d est un diviseur commun à b et r . On a donc $D(a; b) \subset D(b; r)$
 - Considérons d un diviseur commun à b et r .
On sait que $a = b \times q + r$
Comme d divise b et r , on en déduit que d divise a
Donc d est un diviseur commun à a et b . On a donc $D(b; r) \subset D(a; b)$
- On a donc démontré que $D(a; b) = D(b; r)$
Le plus grand élément de $D(a; b)$ est donc aussi le plus grand élément de $D(b; r)$, c'est-à-dire $\text{PGCD}(a; b) = \text{PGCD}(b; r)$

Exemple :

Pour trouver le PGCD de 2414 et 804, on peut écrire la division euclidienne de 2414 par 804 :

On en déduit alors $\text{PGCD}(2414; 804) =$

Il est immédiat que

Propriété : Algorithme d'Euclide

Soit a et b deux entiers naturels non nuls.

On définit la suite r_n d'entiers naturels de la façon suivante :

$$r_0 = b ; r_1 \text{ est le reste de la division euclidienne de } a \text{ par } b$$

- Pour $n \geq 1$:
- si $r_n = 0$ alors $r_{n+1} = 0$
 - si $r_n \neq 0$ alors r_{n+1} est le reste de la division euclidienne de r_{n-1} par r_n

Alors il existe un entier n_0 tel que $r_{n_0} \neq 0$ et pour tout $n > n_0$, $r_n = 0$

On a $\text{PGCD}(a; b) = r_{n_0}$

Preuve :

Soit a et b deux entiers naturels non nuls.

Supposons que pour tout entier n , on a $r_n \neq 0$

Alors pour tout entier n , r_{n+1} est le reste de la division euclidienne de r_{n-1} par r_n

D'après l'encadrement du reste dans une division euclidienne on a $r_{n+1} < r_n$

$$\text{On a alors : } r_1 < r_0 \Rightarrow r_1 < b \Rightarrow r_1 \leq b - 1 \text{ et } r_2 < r_1 \Rightarrow r_2 \leq r_1 - 1 \Rightarrow r_2 \leq b - 2$$

On pourrait alors démontrer par récurrence que, pour tout n , $r_n \leq b - n$

On aurait alors $r_{b+1} \leq b - (b + 1)$ c'est-à-dire $r_{b+1} \leq -1$ ce qui est absurde puisque $r_{b+1} \in \mathbb{N}$

Il existe donc un entier n tel que $r_n = 0$

Considérons l'ensemble E des entiers n tels que $r_n = 0$

Cet ensemble est une partie non vide de \mathbb{N} . Elle a donc un plus petit élément n_1 .

On a donc $r_{n_1} = 0$ et d'après la définition de la suite (r_n) il est immédiat que $r_n = 0$ pour tout $n \geq n_1$

Posons $n_0 = n_1 - 1$

Puisque n_1 est le plus petit élément de E , $n_0 \notin E$ donc $r_{n_0} \neq 0$

De plus si $n > n_0$ on a $n \geq n_1$ et par conséquent $r_n = 0$. On en déduit que $r_n = 0$ pour tout n tel que $n > n_0$

On a vu que lorsque r est le reste non nul de la division euclidienne de a par b , on a $\text{PGCD}(a; b) = \text{PGCD}(b; r)$

En utilisant cette propriété avec les éléments de la suite (r_n) pour $n \leq n_0$ on peut écrire :

$$\text{PGCD}(a; b) = \text{PGCD}(a; r_0) = \text{PGCD}(r_0; r_1) = \text{PGCD}(r_1; r_2) = \dots = \text{PGCD}(r_{n_0-1}; r_{n_0})$$

Comme de plus $r_{n_0+1} = r_{n_1} = 0$, cela signifie que r_{n_0-1} est divisible par r_{n_0} et donc $\text{PGCD}(r_{n_0-1}; r_{n_0}) = r_{n_0}$

On a alors obtenu $\text{PGCD}(a; b) = r_{n_0}$

Remarque :

En effectuant ainsi des divisions euclidiennes successives : de a par b , puis du diviseur par le reste, ... le premier reste non nul est le PGCD de a et de b . C'est l'algorithme d'Euclide. Suivant les nombres a et b , le nombre d'itérations à effectuer peut être plus ou moins grand.

Sachant que $\text{PGCD}(a; b) = \text{PGCD}(b; a)$ on aura toujours intérêt à prendre $b \leq a$

Exemple :

Pour déterminer le PGCD de 410258 et de 126 écrivons les divisions euclidiennes successives :

Pour déterminer le PGCD de 15648 et de 657 écrivons les divisions euclidiennes successives :

C) CONSÉQUENCES DE L'ALGORITHME D'EUCLIDE

Propriété :

Soit a et b deux entiers naturels non nuls.
L'ensemble des diviseurs communs à a et à b est l'ensemble des diviseurs de leur PGCD.

Preuve :

a et b sont deux entiers naturels non nuls . On note $D = \text{PGCD}(a ; b)$

- Soit d un diviseur de D .
 d divise D et D divise a , donc d divise a
 d divise D et D divise b , donc d divise b .
Donc d est un diviseur commun à a et b .
On en déduit que tout diviseur du PGCD est un diviseur commun à a et b .
- Soit d un diviseur commun à a et b . (on peut supposer que $b \leq a$)
 - Si b divise a , alors $\text{PGCD}(a ; b) = b$, donc $D = b$, donc d divise D
 - Si b ne divise pas a .
Écrivons la division euclidienne de a par b , $a = b \times q + r$ avec $0 < r < b$
On a $D = \text{PGCD}(a ; b) = \text{PGCD}(b ; r)$
 - Si r divise b , alors $D = \text{PGCD}(b ; r) = r$,
D'autre part puisque d divise a et b , alors d divise $r = a - b \times q$, donc d divise D
 - Si r ne divise pas b , on peut alors recommencer l'opération.
Or, d'après l'algorithme d'Euclide, on obtiendra $D = \text{PGCD}(r_{n-1} ; r_n)$
avec r_n le dernier reste non nul, c'est-à-dire avec r_n diviseur de r_{n-1} . Donc $D = r_n$
A chaque étape on pourra écrire que d divise r_i et par conséquent d divise r_n .
On aura donc démontré que d divise D .

On en déduit que tout diviseur commun à a et b est un diviseur de leur PGCD.

L'ensemble des diviseurs communs à a et à b est l'ensemble des diviseurs de leur PGCD.

Propriété : Homogénéité

Soit a , b et k trois entiers naturels non nuls.

$$\text{PGCD}(ka ; kb) = k \text{PGCD}(a ; b)$$

Preuve :

Si $a = bq + r$ avec $0 \leq r < b$, alors $ka = kbq + kr$ avec $0 \leq kr < kb$ (car $k \in \mathbb{N}$)

Donc kr est le reste de la division de ka par kb d'après l'unicité de l'écriture.

En utilisant les notations de l'algorithme d'Euclide et multipliant chaque membre des égalités par k , on obtient :

$$\text{PGCD}(ka ; kb) = \text{PGCD}(kb ; kr_0) = \dots = k r_n = k \text{PGCD}(a ; b)$$

2) NOMBRES PREMIERS ENTRE EUX

Exemple :

On voudrait savoir s'il est possible de simplifier la fraction $\frac{1223}{717}$.

Pour cela on peut déterminer le PGCD de 1223 et 717. On trouve $\text{PGCD}(1223 ; 717) = 1$.

Par conséquent les nombres 1223 et 717 n'ont pas de diviseur commun autre que 1 (et -1).

On dit que ces deux nombres sont **premiers entre eux**.

La fraction ne peut pas être simplifiée. On dit que c'est une fraction **irréductible**.

Définition :

Soit a et b deux entiers relatifs non nuls.

On dit que a et b sont **premiers entre eux** si leur PGCD est égal à 1.

Remarques :

- Deux nombres sont donc premiers entre eux s'ils n'ont d'autres diviseurs communs que
- On dit aussi que a est premier avec b , ou que b est premier avec a .
- On dit aussi parfois que a et b sont **étrangers**.

Rappel :

On dit qu'un entier naturel non nul p est premier si ses seuls diviseurs dans \mathbb{N} sont 1 et p .

Propriété :

Soit a un entier relatif non nul.

Si p est un nombre premier qui ne divise pas a , alors $\text{PGCD}(a ; p) = 1$, c'est-à-dire que a et p sont premiers entre eux.
(Si p est un nombre premier, p est premier avec tout entier qui n'est pas un de ses multiples)

Preuve :

p est un nombre premier, donc dans \mathbb{N} l'ensemble des diviseurs de p est $\{1 ; p\}$.

Puisque p ne divise pas a , p n'appartient pas à l'ensemble des diviseurs de a .

Donc dans \mathbb{N} , le seul diviseur commun à p et a est 1 et $\text{PGCD}(a ; p) = 1$.

Exemple :

Démontrons que la fraction $\frac{18866}{13}$ est irréductible.

Propriété :

Soit a et b des entiers relatifs non nuls.

Si $D = \text{PGCD}(a ; b)$, alors $\frac{a}{D}$ et $\frac{b}{D}$ sont des entiers relatifs non nuls premiers entre eux.

(il existe a' et b' deux entiers relatifs non nuls premiers entre eux tels que $a = Da'$ et $b = Db'$)

Preuve :

$D = \text{PGCD}(a ; b)$ alors D divise a et D divise b .

On en déduit qu'il existe a' et b' deux entiers relatifs non nuls tels que $a = Da'$ et $b = Db'$.

Donc $\frac{a}{D}$ et $\frac{b}{D}$ sont des entiers relatifs non nuls.

Soit $d \in \mathbb{N}$ un diviseur commun à $\frac{a}{D}$ et $\frac{b}{D}$, alors

3) THÉORÈME DE BÉZOUT

Théorème de Bézout :

Soit a et b deux entiers relatifs non nuls.

a et b sont premiers entre eux si, et seulement si, il existe deux entiers relatifs u et v tels que $au + bv = 1$.

Preuve :

• Supposons qu'il existe deux entiers relatifs u et v tels que $au + bv = 1$.

• Supposons que a et b sont premiers entre eux.

Considérons l'ensemble E des entiers naturels non nuls de la forme $au + bv$ avec $u \in \mathbb{Z}$ et $v \in \mathbb{Z}$.

E n'est pas vide (E contient a ou $-a$, E contient b ou $-b$, E contient $2a + 3b$ ou $-2a - 3b \dots$), donc E a un plus petit élément m .

On peut écrire $m = au_1 + bv_1$ avec $u_1 \in \mathbb{Z}$ et $v_1 \in \mathbb{Z}$.

Écrivons la division euclidienne de a par m : $a = mq + r$ avec $r \in \mathbb{N}$ et $0 \leq r < m$.

On a alors : $a = (au_1 + bv_1)q + r \Rightarrow r = a - (au_1 + bv_1)q \Rightarrow r = a(1 - u_1q) + b(-v_1q)$

Donc r est un entier naturel de la forme $au + bv$ avec $u \in \mathbb{Z}$ et $v \in \mathbb{Z}$ et d'autre part $r < m$.

Comme m est le plus petit élément de E , on en déduit que $r = 0$, c'est-à-dire que a est divisible par m .

De même on démontrerait que b est divisible par m .

Donc m est un diviseur commun à a et b .

Comme a et b sont premiers entre eux, on en déduit que $m = 1$.

On a donc $1 = au_1 + bv_1$ avec $u_1 \in \mathbb{Z}$ et $v_1 \in \mathbb{Z}$.

Remarque : Le théorème de Bézout est particulièrement intéressant pour travailler sur des expressions littérales ou sur des grands nombres.

Exemple :

En utilisant l'algorithme d'Euclide démontrons que 383 et 127 sont premiers entre eux et déterminons des entiers relatifs u et v tels que $383u + 127v = 1$

	Pour déterminer u et v , l'idée est d'exprimer le 1 qui apparaît comme reste de la dernière division en fonction des nombres 383 et 127.
On peut écrire $383 = 127 \times 3 + 2$ (1) et $127 = 2 \times 63 + 1$ (2)	D'après l'égalité (1), on peut écrire D'après l'égalité (2), on peut écrire En remplaçant 2 par $383 - 127 \times 3$ dans l'égalité (3), on obtient :
Donc $\text{PGCD}(383 ; 127) = 1$ c'est-à-dire que 383 et 127 sont premiers entre eux.	

On peut donc prendre $u = -63$ et $v = 190$.

Le couple $(u ; v)$ d'entiers relatifs n'est pas unique, on peut vérifier que les couples $(64 ; -293)$ et $(-317 ; 956)$ répondent aussi à la question.

Propriété :

Soit a, b des entiers relatifs non nuls et D un entier naturel non nul. Les propositions si-dessous sont équivalentes :

- $D = \text{PGCD}(a ; b)$
- $\frac{a}{D}$ et $\frac{b}{D}$ sont des entiers relatifs non nuls premiers entre eux.
- $a = Da'$ et $b = Db'$ a' et b' étant deux entiers relatifs non nuls premiers entre eux.

Preuve :

Soit a, b des entiers relatifs non nuls et D un entier naturel non nul.

- On a déjà vu que si $D = \text{PGCD}(a ; b)$, alors $\frac{a}{D}$ et $\frac{b}{D}$ sont des entiers relatifs non nuls premiers entre eux.
- Supposons que $\frac{a}{D}$ et $\frac{b}{D}$ sont des entiers relatifs non nuls premiers entre eux.
Puisque $\frac{a}{D}$ et $\frac{b}{D}$ sont des entiers, D divise a et D divise b .
Soit $g = \text{PGCD}(a ; b)$.
 D divise a et b , donc D divise g et donc $D \leq g$.
D'autre part $\frac{a}{D}$ et $\frac{b}{D}$ sont premiers entre eux, donc il existe des entiers relatifs u et v tels que $\frac{a}{D}u + \frac{b}{D}v = 1$, c'est-à-dire $D = au + bv$.
Mais g étant le PGCD de a et de b , g divise a et b , donc g divise $au + bv$ donc g divise D , donc $g \leq D$.
On a donc finalement $g = D$, c'est-à-dire $D = \text{PGCD}(a ; b)$.
On a donc démontré l'équivalence des deux premières propositions.
- L'équivalence des deux dernières propositions est immédiate.

Théorème de Bézout généralisé : Caractérisation du PGCD

Soit a, b des entiers relatifs non nuls et D un entier naturel non nul.
 $D = \text{PGCD}(a ; b)$ si et seulement si D divise a et b et s'il existe deux entiers relatifs u et v tels que $au + bv = D$.

Preuve : exigible

•

•

Remarque :

La condition D divise a et b est importante . Par exemple $7=4\times 1+3\times 1$, mais 7 n'est pas le PGCD de 4 et 3

4) THÉORÈME DE GAUSS

Théorème de Gauss :

Soit a et b deux entiers relatifs non nuls et c un entier relatif.
Si a divise bc et si a est premier avec b , alors a divise c .

Preuve : exigible

Soit a et b deux entiers relatifs non nuls et c un entier relatif tels que a divise bc et a est premier avec b .
 a et b sont premiers entre eux, il existe donc des entiers relatifs u et v tels que $au + bv = 1$.

Propriété : (parfois appelé théorème d'Euclide)

Soit a et b deux entiers relatifs et p un nombre premier.
Si p divise le produit ab , alors p divise a ou p divise b .

Preuve :

Soit a et b deux entiers relatifs. On suppose que p est un nombre premier divisant le produit ab .

Supposons que p ne divise pas a , alors $a \neq 0$ et a et p sont premiers entre eux (puisque p est premier)

Donc p divise ab et p est premier avec a , donc p divise b . (Théorème de Gauss)

Propriété :

Soit a et b deux entiers relatifs non nuls premiers entre eux et soit n un entier naturel.
Si n est divisible par a et par b , alors n est divisible par le produit ab .

Preuve :

Soit a et b deux entiers relatifs non nuls premiers entre eux, et n un entier naturel tel que n est divisible par a et par b .

a et b sont premiers entre eux, il existe donc des entiers relatifs u et v tels que

On a alors

On sait que a divise n , donc $n = aq$ avec $q \in \mathbb{Z}$ et b divise n , donc $n = bq'$ avec $q' \in \mathbb{Z}$.

L'égalité $na + nbv = n$ peut alors s'écrire .

Alors ab divise ab divise donc ab divise c'est-à-dire ab divise

Exemple :

Si un nombre est divisible par 5 et par 6, alors